SheppardMullin

Sheppard Mullin Richter & Hampton LLP
30 Rockefeller Plaza
New York, NY 10112-0015
212.653.8700 main
www.sheppardmullin.com

212.634.3092 direct
randoh@sheppardmullin.com
File Number: 02HL-350124

April 19, 2022

FILED VIA ECF

Hon. Jeremiah J. McCarthy mccarthy@nywd.uscourts.gov
Deputy Clerk: Eric Glynn
United States Magistrate Judge
Robert H. Jackson United States Courthouse
2 Niagara Square
Buffalo, NY 14202

Re: *Moog Inc. v. Skyryse, Inc., et al.*
U.S. District Court, Western District of New York – Case No. 1:22-cv-00187

Dear Honorable Judge McCarthy:

We are counsel for plaintiff Moog Inc. ("Moog") in the above-referenced matter. Pursuant to the Court's directives following the April 8, 2022 Conference (ECF Nos. 57, 58, 72), Moog hereby submits its letter brief regarding three outstanding issues that were raised in Moog's initial April 6, 2022 email submission to the Court, and that were not resolved with Defendants after additional meet and confer correspondence:

1. Defendants' non-compliance with the March 11, 2022 Stipulation and Order (the "March 11 Order") regarding return and non-use of Moog Confidential Information;

2. the framework for a protocol that will govern inspection of materials turned over to neutral forensic vendor iDiscovery Solutions ("iDS"), including 25 devices turned over to iDS by the Defendants pursuant to the March 11 Order; and

3. the scope of disclosure of materials designed "Attorneys' Eyes Only" ("AEO") under the stipulated protective order being negotiated by the parties.

I. Defendants' Failure to Comply with the March 11 Order

On April 6, 2022, Skyryse's counsel unequivocally stated in a letter to counsel for Moog: "***Skyryse fully complied with its obligations under the March 11 Order***." In its April 7 letter to Judge McCarthy, Moog laid out many of the reasons why it had (and continues to have) grave concerns that Skyryse is not in compliance with its obligations under the March 11 Order, which required it to "return to Plaintiff any and all … non-public information, documents, records, files, or data in [] Defendant's possession, custody, or control…." In the April 7 letter, Moog asked for specific relief, namely "requiring Defendants to explain in writing, within seven days, the steps taken to:

- Search Skyryse's systems for any Moog data [] transferred from any of the 23 electronic devices turned over by Pilkington and Kim's counsel;

- Search Skyryse's devices or systems for Moog data transferred from any personal devices of the other 20 former Moog employees employed at Skyryse (or at a minimum, the 15 non-party former Moog employees who departed after Pilkington); [and]

- Search for any of the 1.2 million files copied by Pilkington, or investigate the two separate hard drives involved in those acts of copying."

During the conference with Judge McCarthy on April 8, counsel for Skyryse expressly stated: "So as to the specific requested relief in Moog's letter, item three which had those different bullets, we're happy to do what they have asked and to provide that information." (*See* ECF 71 (4/8/22 Hrg. Tr.) at 15:10-12). Yet Skyryse sent a letter to Moog on Friday, April 15, that demonstrated Skyryse did *not* follow through with its representation to the Court. The letter, instead, demonstrated the following:

- Skyryse to date has not reviewed—nor coordinated with counsel for the individual defendants to obtain information regarding—any of the 23 electronic devices turned over by the individual defendants containing Moog non-public information;

- While Skyryse said it ran the filenames provided by Moog in connection with the Kim downloads across its Google Drive document repository, which "produced some matches," and that they are "reviewing the contents of the resulting hits," they have not reviewed any of the personal or work devices of the other 18 former Moog/current Skyryse employees.

- ***Skyryse to date has not made any attempt to review any Skyryse systems or individual defendant devices for any of the 1.2 million files Pilkington took***.

(*See* enclosed Appendix of Exhibits ("Appx"), Ex. C). Skyryse further refused to provide a list of the file names of documents that have hit as a result of searches Skyryse performed, even though there are at least three sets of searches that have hits that Moog is aware of to date: (1) one set of 11,000+ files; (2) one set of undetermined size because Skyryse refused to disclose the number; and (3) one subset of at least 100 files that contain the word "Moog" in them. As a result, it is impossible for Moog to review the files for itself and determine whether any of them are Moog's non-public information or not. Moreover, in response to a request from Skyryse and to try and provide additional assistance, Moog provided an additional 32 search terms to Skyryse on April 12, but Skyryse has apparently run *none* of these keywords across their systems or devices.[1] Skyryse refuses to turn any of this information over notwithstanding Skyryse counsel's representation to the Court that "we're happy to be transparent about what we're doing because we feel that strongly that we don't want the material and we don't want there to be any suggestion

[1] Moog, however, made clear that those search terms are not close to a complete solution as far as identifying evidence of possession or misappropriation, because copying of Moog data would surely have been followed by a deliberate replacement of distinctive Moog terms in order to obfuscate the theft, or to adapt the copied data to Skyryse's systems. Additionally, search terms would not capture misappropriation whereby Defendants reference Moog files in order to adapt processes, architecture, designs, etc., without necessarily verbatim word-for-word copying.

that we are not fully complying not only with the various orders Judge Vilardo has entered, but just generally our commitment to return any Moog confidential information that we have." (ECF 71 at 14:6-12).

In sum, Skyryse has not undertaken a sufficient search to find and return Moog's non-public materials, despite more than two weeks having elapsed since the deadline articulated in the March 11 Order. Moreover, the process of repeatedly confronting Skyryse over its lack of compliance is time consuming and unlikely to be fruitful given Skyryse's total lack of transparency. It is unsurprising that non-compliance has been Skyryse's strategy, since any identification of Moog non-public information on Skyryse's systems would provide strong circumstantial evidence of use, and is thus not in Skyryse's best interest in defending itself in this action. Therefore, instead of continuing to focus on compelling Skyryse to provide more information about its search for Moog non-public information, the most efficient and viable path forward is for Moog's retained experts and outside counsel to gain access to forensic images of all the devices Defendants turned over, and let them conduct a real investigation, as explained in Section II. For this reason, it is critical that any protocol approved by the Court relating to the 25 devices currently in escrow with the neutral forensic firm is to permit Moog's retained experts and outside counsel to have access to forensic images of those devices.

II. The Parties' Dispute Regarding the Forensic Inspection Protocol

The parties have fundamental disagreements about the overall framework of the protocol that would govern inspection of materials that have been or will be turned over to the neutral forensic vendor iDS (the "Inspection Materials"), including 25 devices that Defendants have collectively turned over because they presumptively contain Moog data.[2] Moog requests a protocol that permits its retained experts and outside counsel (but not any Moog personnel) to inspect forensic images of the Inspection Materials—after a reasonable review period for Defendants to remove privileged material.[3] Moog believes this is the only protocol framework that will result in a full and effective investigation into the extent of Defendants' misappropriation. Moog's proposed protocol is attached to the Appendix as **Exhibit A**.

Defendants, by contrast, want a protocol that erects a wall between Moog and the Inspection Materials and hobbles Moog's and the Court's ability to uncover the full scope of Defendants' misappropriation. Specifically, Defendants want a protocol that permits only the neutral forensic vendor iDS to inspect the forensic image—Moog's retained experts and outside counsel would get no access. Moreover, under Defendants' proposed protocol, iDS can only

[2] Skyryse turned over two devices, Ms. Kim's Skyryse-issued computer and an external hard drive. The individual defendants Alin Pilkington and Misook Kim turned over 23 devices, including computer devices and external hard drives. One of the hard drives turned over by Ms. Kim matches the description of a hard drive used by Ms. Kim to improperly download a number of files from Moog prior to her departure.

[3] A "forensic image" (sometimes called a "mirror image") of a device is described as a "forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space, including slack space, on a computer hard drive." *Commc'ns Ctr., Inc. v. Hewitt*, No. 03-cv-1968, 2005 WL 3277983, at *1 (E.D. Cal. Apr. 5, 2005).

search for exact names of the files that were stolen, and "hash values" corresponding to the stolen files.[4] Defendants' protocol provides for no other way to search for misappropriating use, such as copying of only portions of a file, or copying that is later obfuscated by the replacement of distinctive words, and so forth. Additionally, Defendants' proposed protocol does not contemplate analysis of metadata, access logs, and other "forensic data" regarding the 25 devices they turned over. Defendants' proposed protocol is attached to the Appendix as **Exhibit B**.

Moog requests that the Court enter Exhibit A as the inspection protocol in this case.

A. Permitting Moog's Retained Experts and Outside Counsel to Directly Inspect the Forensic Images Is Proper

As a general matter, it is proper for a defendant in a trade secret case to permit a plaintiff's retained experts and outside counsel to directly inspect forensic images of the defendant's devices, so long as the defendant is provided a reasonable opportunity to remove privileged documents. *See Allergan, Inc. v. Merz Pharms., LLC*, No. 11-cv-00446, 2011 WL 13323241, at *4 (C.D. Cal. June 9, 2011) (ordering in a trade secret misappropriation case that "Individual Defendants shall provide to Plaintiff forensic images of each of the media in question, subject to the opportunity of the Individual Defendants to eliminate any material for which a privilege or other objection to production is claimed"); *id.* at *3 (finding that the "balance [of interests] can best be achieved by allowing Plaintiff direct access to the forensic images of the media in question, consisting of hard drives and external storage media" and permitting defendants to "identify[] and excis[e] the objectionable material, together with creating a reasonably detailed log of those materials deleted and why"); *BalanceCXI, Inc. v. Int'l Consulting*, No. 19-CV-0767, 2020 WL 7034123, at *1–2 (W.D. Tex. Nov. 24, 2020) (ordering in a trade secret case that to the extent plaintiff "requests the laptop for examination in the future," plaintiff may employ a protocol whereby the "laptop [is] imaged" and plaintiff may conduct "examination of the Image"); *Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *10 (E.D. Va. Dec. 5, 2003) (ordering in trade secret theft case that plaintiff is permitted to "enter the sites where the computers used in the alleged attacks are located and to obtain a 'mirror image' of the computer equipment containing electronic data relating to Defendants' alleged attacks on Physicians Interactive's file server"); *see also Audio Visual Innovations, Inc. v. Burgdolf*, No. 13-10372, 2014 WL 505565, at *3–4 (E.D. Mich. Feb. 3, 2014) (ordering in a trade secret case that forensic vendor provide list to both parties' counsel of all files on the device, including deleted files, that the defendant's counsel identify the files it seeks to excise for being objectionable in the form of a log, which the plaintiff's counsel has the right to challenge, and that *all other files* be produced to the plaintiff on a default AEO basis unless and until the parties confer on a different designation).

Privilege Concerns Will Be Adequately Addressed

Moog's proposed protocol permits Defendants to review the Inspection Materials for privileged documents and excise those within a prompt amount of time after entry of the protocol,

[4] A "hash value" is a "unique numeric identifier for [a] digital computer file[]." *United States v. Heleniak*, No. 14-CR-42A, 2015 U.S. Dist. LEXIS 89728, at *3 (W.D.N.Y. July 10, 2015). Where even a single bit or character is changed in a file, the hash value generated from that file will no longer match the original. *See id.*

in order to prevent undue delay in light of the expedited discovery schedule and preliminary injunction hearing; Defendants would also identify what was excised with reasonable particularity in a log. This is proper. *See Allergan*, 2011 WL 13323241, at *4 ("For any such material eliminated, the Individual Defendants shall provide at the time of the production of the image in question a log identifying the eliminated material with reasonable particularity, along with a brief statement of the reason for eliminating it. The identification should contain, so far as reasonably possible, the identification of the location on the media of the eliminated material.").

Moog does not expect the amount of privileged material or the burden on Defendants to be significant. The 25 devices Defendants turned over relate chiefly, if not entirely, to Pilkington and Kim. *See* fn. 2, *supra*. Pilkington and Kim are engineers, not lawyers, and thus Moog does not expect the devices to contain significant amounts of privileged communications or attorney work product. They also only worked for Skyryse for brief periods of time prior to the devices being turned over: Pilkington from mid-November of 2021, and Kim from January of 2022. What privileged documents do exist on these devices are likely discrete, i.e., involving a discrete group of lawyers (e.g., from the Gibson Dunn and Locke Lord law firms, for instance), a discrete group of issues (e.g., pertaining to this lawsuit), and a discrete time frame (within the last few months)—meaning that any burden from identifying potential privileged documents is minimal. Moreover, any burden from privilege review is reasonable for Defendants to bear. "Fundamental to this aspect of the law," i.e., privilege, is that "the party claiming the privilege has the burden of establishing and protecting it." *Allergan*, 2011 WL 13323241, at *2; *id.* at *3 ("It is understood that [the privilege review] will be burdensome to the Individual Defendants. However, it is they who have interposed the objections. . . . [I]dentifying allegedly objectionable material[] [] should be the burden of the objecting party."). Second, for Defendants to bear the burden here is especially appropriate because it is they who undisputedly stole over 1.3 million files from Moog. Defendants cannot now use the volume of their theft as a shield against privilege review or direct inspection generally.

The Inspection Would Be Subject to the Protective Order and Restricted

Defendants have argued that Moog's retained experts and outside counsel should not be given "unfettered" access to the forensic images of the devices because they may contain Skyryse's "highly confidential and trade secret information." But these objections lack merit for at least the following reasons. First, the access will not be "unfettered" but instead subject to the protections of the Protective Order, and outside counsel in particular are officers of the Court. Second, only two of the 25 devices were handed over by Skyryse—the remaining 23 were handed over by Pilkington and Kim personally, and Skyryse has given no indication that these devices would contain Skyryse information. And third, Moog's retained experts and outside counsel will not have physical possession of the forensic images—only iDS will. (*See* Exhibit A, § III.A.) iDS will host the forensic images on its own servers, called a "virtual machine" in Moog's proposed protocol. (*See id.*, § III.B.) Moog's retained experts and outside counsel will only be able to access the forensic images on iDS's virtual machine by using secure laptops (managed by iDS) in a secure environment. (*See id.*, § III.D.) The review of the forensic images by Moog's retained experts and outside counsel will also be monitored by iDS. (*See id.*, § III.E.)

To be clear, Moog's retained experts and outside counsel have no interest in Skyryse's so-called "highly confidential and trade secret information." But they do need to inspect Skyryse's

documents to investigate the extent to which they incorporate *Moog's* trade secrets from over 1.3 million files that Skyryse's employees have undisputedly stolen. That these Skyryse documents may incidentally contain Skyryse's purported "highly confidential and trade secret information" is not sufficient reason to block Moog from conducting a full and fair investigation (one that Defendants are unwilling or unable to undertake, *see* Section I). It was Defendants who created this mess, and per the March 11 Order, the 25 devices they turned over *presumptively* contain Moog data. Ironically, Defendants seek to block Moog's retained experts and outside counsel from access to devices purportedly containing Skyryse's highly confidential information; yet they seek to give Skyryse's *employees* Pilkington and Kim access to all of Moog's highly confidential information—despite Moog having legitimate concerns regarding their trustworthiness. (*See* Section III, *infra*.) Defendants' position is hypocritical, unfair, and improper.

Defendants' Authorities Are Distinguishable

Defendants cited three decisions during the course of the parties' meet and confer to support their position—*Calyon v. Mizuho Sec. USA Inc.*, No. 07-cv-02241, 2007 WL 1468889 (S.D.N.Y. May 18, 2007), *Henson v. Turn, Inc.*, No. 15-cv-01497, 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018), and *Moser v. Health Ins. Innovations, Inc.*, No. 17-cv-1127, 2018 WL 6735710, at *6 (S.D. Cal. Dec. 21, 2018)—but all three are distinguishable.

First, *Calyon, Henson,* and *Moser* are not cases involving trade secret claims. *See Calyon*, 2007 WL 1468889, at *1 n.2 (instead involving claims of breach of fiduciary duty, unfair competition, tortious interference with business relationships, and others); *Henson*, 2018 WL 5281629, at *1 (involving data privacy class action claims); *Moser*, 2018 WL 6735710, at *1 (involving TCPA class action claims). Cases involving claims of theft of trade secrets, however, are more likely to merit direct inspection by a plaintiff of forensic images of devices, especially where those devices contain the electronic materials that were stolen or misappropriated. *See Balboa Threadworks, Inc. v. Stucky*, No. 05-cv-1157, 2006 WL 763668, at *3 (D. Kan. Mar. 24, 2006) (distinguishing itself from trade secret cases, because "where trade secrets and electronic evidence are both involved, the Courts have granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation"). As further explained below, none of *Calyon*, *Henson*, or *Moser* involve a defendant's theft of over 1.3 million of the plaintiff's files (as has occurred here); none of these cases involve the plaintiff's request to inspect devices that were turned over by defendants pursuant to a *stipulated* temporary restraining order because they contain the *plaintiff's* stolen information, (as has occurred here); and none of these cases involve a defendant who has indisputably spoliated (i.e., destroyed and deleted) nearly 137,000 stolen files (as has occurred here).[5]

[5] We would note, however, that direct inspection of devices has been granted to a plaintiff even in cases not involving theft of the plaintiff's own trade secrets. *See, e.g., Forreststream Holdings Ltd. v. Shenkman*, No. 16-cv-01609, 2018 WL 6522218, at *6 (N.D. Cal. Dec. 11, 2018) (ordering that plaintiff's outside counsel be permitted to make a forensic image of defendant's laptop and review it directly, after defendant had the opportunity to remove privileged documents subject to providing a log of all removed documents, in order for plaintiff to discover information to satisfy a judgment against defendant).

In *Calyon*, the court specifically found that "[Plaintiff has not] argued that the Individual Defendants have made any representation that relevant documents or data have been lost, such that there may now be a need for [plaintiff] to conduct a more exhaustive electronic search in order to try to find that information. Nor has [plaintiff] identified any specific information that it seeks to recover from the mirror images, and shown that the Individual Defendants would not be capable of, or willing to, produce that particular information. In sum, the Court is not yet faced with any failure by the defendants to conduct a thorough forensic search of their computers, or to produce any and all relevant documents, files, metadata, and even hidden data fragments that [plaintiff] may request." *Calyon*, 2007 WL 1468889, at *5. However, all of these concerns are very much present here, unlike in *Calyon*:

- "Relevant documents or data" *have* been lost here. Kim deliberately formatted the Moog hard drive that she stole, wiping the drive completely clean, *before* returning that drive to Moog. (Compl., ¶¶ 132. 137). In other words, she deliberately deleted all of the nearly 137,000 Moog files that she copied onto that drive, and destroyed all forensic data pertaining to those copied files (i.e., when she copied, accessed, edited, or destroyed the files). (*Id.*). Moog therefore has ample reason to believe that further spoliation has occurred on the 25 devices Defendants have turned over to iDS.

- Moog *has* identified specific information that it seeks to recover from the mirror images. For example, Moog seeks to recover forensic data regarding the devices (i.e., when the devices were connected to other devices, when files were deleted from or copied to the devices, when particular files were accessed on the devices, and so forth, *see* Section II.B.3, *infra*). As another example, Moog also seeks to review *at least* source code, other technical documents, and process assets. (*See* Section II.B.1 & II.B.2, *infra*). Finally, these categories of documents are just examples of documents that Moog believes would reflect misappropriation—Moog's retained experts and outside counsel need to inspect the forensic images precisely because they do not yet know all the categories of documents that would reflect misappropriation, and need to discover that.

- The Defendants' conduct so far in this case have shown that they "would not be capable of, or willing to, produce" information needed for an adequate investigation of their misappropriation, and the Court here is in fact faced with "failure by the defendants to conduct a thorough forensic search of their computers, or to produce any and all relevant documents, files, metadata, and even hidden data fragments that [plaintiff] may request." (*See* Section I, *supra*).

The *Henson* case is also distinguishable on further grounds. In *Henson*, the court found that permitting defendants direct access to the forensic image of plaintiff's personal device was inappropriate when defendants were specifically accused of breaching plaintiff's privacy to begin with. *Henson*, 2018 WL 5281629, at *8 ("There is an Orwellian irony to the proposition that in order to get relief for a company's alleged surreptitious monitoring of users' mobile device and web activity, a person has to allow the company unfettered access to inspect his mobile device or his web browsing history. Allowing this discovery would further invade the plaintiffs' privacy interests and may deter current and future plaintiffs from pursuing similar relief."). Here, we have the reverse situation—plaintiff needs access to forensic images of devices because the *defendants* have stolen *plaintiff*'s confidential data and have obstructed plaintiff's investigation

into this theft, including by destroying and spoliating nearly 137,000 files. *Defendants* are the ones who, through their misappropriation, created the situation the parties are in, and cannot now be heard to unreasonably limit Moog's access to the very devices containing Moog data.

In *Moser*, like in *Calyon*, the court noted that direct access may be appropriate if there is a finding of "improper conduct on the part of the responding party or intentional destruction of relevant electronic evidence." *Moser*, 2018 WL 5281629, at *6 (internal quotations omitted). Here, there can be no question of improper conduct—Defendants *stipulated* to a temporary restraining order because they concede that Moog files have been taken by at least two Skyryse employees (Kim and Pilkington); and it is *undisputed* that Kim intentionally destroyed relevant electronic evidence, i.e., the nearly 137,000 files that she copied onto a Moog-issued external hard drive that she took with her to Skyryse.

And in both *Henson* and *Moser*, the court found that direct access to the forensic image of the entire devices was disproportionate to the needs of the case because the actual information sought by the defendant was very limited—namely, records relating to "cookies" (which "monitor and gather information about users' browsing and app use") in *Henson*; and records relating to phone and website activity in *Moser*. *Henson*, 2018 WL 5281629, at *1; *Moser*, 2018 WL 5281629, at *6. By contrast here, the reason Moog needs direct access is because of the enormous *breadth* of materials that require review on those devices. Defendants have stolen over 1.3 million of Moog's files, covering a huge array of Moog's intellectual property, and the ways in which the data in those files could have been misappropriated is virtually limitless. Moog needs direct access (for its retained experts and outside counsel) in order to investigate the scope, breadth, and depth of the misappropriation.

Moreover, in all of *Calyon*, *Henson*, and *Moser*, the parties objecting to direct inspection chiefly had privacy concerns. Here, Defendants never raised privacy as a concern even once throughout the meet and confer process. However, to the extent Defendants raise it for the first time in their submission, it is no excuse for blocking Moog's direct inspection. First, Defendants can screen for any privacy concerns at the same time that they screen for privilege. Second, as to the two devices Skyryse turned over, those are company devices and presumably should not contain significant amounts of personal data. Third, as to the 23 devices Pilkington and Kim collectively turned over, to the extent they are personal devices, the fact they copied Moog data onto the devices and departed with them is not only theft of the Moog data but a breach of Moog company policy. (*See* Appx. Ex. D, p. 8, § 10.13 (Moog's Acceptable Use Policy, which provides,

REDACTED

Defendants cannot now use that same breach and misconduct—i.e., use of personal devices to copy and steal Moog data—to now block Moog's retained experts and outside counsel from inspecting those devices for misappropriation. This is especially true where information on the devices would only be disclosed to Moog's outside counsel and retained experts under a "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL & EXPERTS' EYES ONLY" designation.

B. Defendants' Proposed Limitations Are Improper and Not Suitable for This Case

The insufficiency of Defendants' proposed approach—i.e., limiting inspection access to only iDS and limiting search parameters to just file names and hash values—is readily demonstrated by examination of how such limitations would adversely impact the inspection of three categories of materials pertaining to the devices, as explained below: (1) source code and other technical documents; (2) process assets; and (3) forensic data regarding devices.[6]

i. Source Code and Other Technical Documents

(1) Limiting inspection to search of file names and hash values is insufficient.

Defendants have collectively stolen over 1.3 million documents, a significant amount of which was source code and other technical documents, from projects such as eRTOS, Platform, and so forth. We expect that the wholesale further copying of these files, unaltered, by Skyryse employees onto Skyryse's network or other Skyryse devices to be just a slim minority of Skyryse's misappropriating use of these files, for at least several reasons. One is that a significant number of these files contain Moog proprietary statements, e.g., statements with headers like "MOOG PROPRIETARY AND CONFIDENTIAL INFORMATION." Moog does not expect Skyryse employees to wholesale copy a file, unaltered, because the inclusion of the Moog proprietary statement would make the theft too obvious. Another reason is that a whole file (as opposed to just portions of a file) may be more difficult to "plug" into the existing Skyryse projects or systems.

Instead, Moog suspects the vast majority of Skyryse's misappropriation to involve Skyryse employees treating source code and other technical documents as more of a "reference library" as they are developing Skyryse processes and products. For example, Skyryse employees are likely to pick and choose portions from the Moog "reference library" (e.g., a function here, a function there) to copy or incorporate into Skyryse documents, carefully excluding portions with the term "Moog" in them such as the Moog proprietary statement, and replacing names and terms distinctive to Moog in order to obfuscate the theft.[7] Skyryse employees are also likely to use Moog files as a visual reference while they draft Skyryse documents—for example, using the same algorithms, structures, process flows, etc., but using different words to implement the foregoing (in order to, among other things, obfuscate the theft).

Searching for exact file names and hash values corresponding to the stolen files is useless to identify these types of misappropriation. Indeed, the inadequacy of searching for file names and hash values has been demonstrated and proven during the TRO process—Defendants have

[6] To be clear, these three categories are provided as examples only and are not limiting.

[7] Using a litigation analogy, if someone were to plagiarize a brief, one would not expect that person to just pull the brief from PACER and then file it with the Court. The plagiarism would be too obvious, and the brief would not likely fit with the case. Instead, one would expect that person to pick and choose portions from the brief that he likes, discarding the rest, and incorporate the plagiarized portions into his own brief template and caption.

employed this very technique and failed to adequately identify the stolen materials and comply with the TRO.

Moreover, Moog does not even have accurate hash values to give to Skyryse, due to Defendants' own misconduct. Among other things, because Kim completely wiped the Moog-issued hard drive containing the nearly 137,000 files she stole, those files are no longer in existence from which to generate hash values. The best Moog could do was search for files on Kim's Moog-issued laptop that *might* correspond to the nearly 137,000 files, which is itself largely impossible because Kim also deleted thousands of files from her Moog-issued laptop to cover up her copying and theft. The only individuals who potentially have accurate hash values are Kim and Pilkington (and anyone else to whom they passed on the copied data), because they are the ones who took the files from which the hash values can potentially be generated. Yet, Defendants have placed the entire burden on Moog to identify hash values for the files that *they* stole without having access to the most likely locations on which the files still exist—the 25 devices Defendants turned over. It is a classic Catch-22.

For the above reasons, searching for hash values and file names is not nearly adequate for the investigation that is needed in this case. Instead, having Moog's retained expert review the source code and technical documents directly through visual inspection, comparing them side-by-side with Moog's own documents where appropriate, and exercising his judgment based on his relevant technical expertise and experience in aviation software development, is the appropriate way forward. *See HP Tuners, LLC v. Cannata*, No. 18-CV-00527, 2020 WL 4905533, at *2 (D. Nev. Aug. 20, 2020) (ordering in trade secret misappropriation case that "Forensic Examiner identified by Plaintiff . . . shall make a mirror image of Defendant's Electronic Devices [and] shall also be permitted to review, inspect and analyze[] . . . any and all firmware, software and source code (including all source control, changelogs and/or the history of all modifications to such firmware, software, and source code) in Defendant's possession, custody or control related to automotive tuning software, hardware and/or products developed or sold by Plaintiff").[8]

(2) Moog's Retained Expert Can Conduct the Inspection Necessary, Not the Neutral Forensic Vendor

As explained above, the misappropriating use of source code and other technical documents that is at the heart of this case and described above cannot be adequately identified using merely file names or hash values (as Defendants have proposed) or other search terms. These mechanical, superficial, brute force methods will not work. Instead, conducting an adequate inspection requires a more sophisticated, nuanced approach, executed by someone with expertise in aviation software development. For example, the retained expert must analyze how Skyryse's flight control software is architected and the extent and nature of that architecture's similarities to Moog's, including by visually comparing code side-by-side where necessary. As another example, the retained expert must know what the relevant source code looks like, analyze Skyryse's repository logs to identify large check-ins of such source code, and exercise judgment

[8] On the parties' meet and confer, Defendants' counsel seemed to float the possibility of searching for keywords in addition to file names and hash values. But searching for keywords is also insufficient, for reasons identified above. (*See* fn.1, *supra*).

based on experience to determine whether such check-ins are unusual and atypical in aviation software development.

iDS does not have the above expertise. (*See* Appx. Ex. E (information from iDS's website, showing that they do not identify as experts in aviation software development, or even software development generally)). While iDS has adequate expertise to serve as an "escrow" agent for the devices and to forensically image those devices for Moog's inspection, iDS does not have expertise in aviation software development. This is why Moog intended for iDS to forensically image the devices and host those forensic images for inspection, and that iDS would host source code review for the case. Moog never proposed or agreed to iDS with the intent that they would serve in the role of reviewer and inspector of materials. Indeed, none of the parties raised these capabilities with iDS during the vetting process and communications with iDS prior to engaging iDS on April 1. The March 11 stipulated TRO expressly leaves the details of who will conduct the inspection and how the inspection will be conducted unaddressed, instead stating generally that the parties shall "agree on a protocol for searching all such information delivered to the Forensics Firm." (Dkt. 25, p. 3). It does *not* say, for example, that the parties shall "agree on a protocol for searching ***by the Forensics Firm of*** all such information delivered to the Forensics Firm." And certainly, it was never Moog's intent that the "Forensic Firm" do so. Instead, Moog's intent was that the "Forensics Firm" host the data securely, so that none of the parties take possession of the devices in the first instance, and make proper forensic images of the devices for the parties' inspection. Nor does the stipulation say that the parties shall "agree on a protocol for searching ***for file names and hash values in*** all such information delivered to the Forensics Firm." The foregoing said, if *Defendants* want to solely use iDS to search materials using file names and hash values for the purpose of their defense, that is Defendants' choice. But Moog will not be deprived of its choice of expert or reasonable methods of inspection to adequately prosecute its case.

Further to this point, on the parties' meet and confer on April 7, Defendants repeatedly suggested *they* lacked the capability and understanding to conduct the necessary inspection in this case, asking repeatedly for *Moog* to identify what they could search for besides file names and hash values. iDS is far further removed from this case than the Defendants are, underscoring why iDS cannot undertake such an inspection on a substantive basis.

ii. Process Assets

The insufficiency of Defendants' proposed protocol is also demonstrated by examination of another category of materials on the devices, i.e., process assets.

In addition to source code and related technical documents, Defendants also stole Moog's repository of process assets, e.g., templates, checklists, tools, test cases, artifacts,[9] etc. pertaining to compliance with FAA regulations, in particular DO-178. As Defendants know, the development of flight software hinges on compliance with DO-178, a government standard that a company must follow in order to develop software for use in FAA airspace. Moog has spent years

[9] An "artifact" as used here is a completed checklist that proves the company has reviewed the source code at issue and that the code is correct, which would be presented to the FAA in the case of an audit.

developing the process assets to ensure compliance with DO-178. This includes a large template library, for example, that sets the framework for software development that is compliant with DO-178 and FAA safety requirements, and which would be used in the compliance approval and certification process. In fact, because Moog develops software at the highest level of criticality, much more time is spent on testing, reviews, and development of documentation that support the artifacts to show that the code complies with DO-178, than on the code itself. These process assets take years to develop.

Moog believes Skyryse is particularly interested in these extremely valuable process assets because Skyryse is seeking DO-178 compliance certification, but did not (prior to the theft and poaching of Moog employees) have background or experience in this area. For example, while at Moog, Pilkington developed a Python-based qualification tool for automated verification called MDTE (Moog Desk Top Environment), which follows the DO-330 standard. This tool is used to test flight software in connection with DO-178 compliance certification. This tool is valuable because it automates the verification process (which, as explained above, constitutes the majority of time spent by Moog on software development) and therefore saves time and money. By stealing this tool and either referencing the tool or copying portions of it, Skyryse is able to fast-track what would otherwise take years to develop, especially given its own (prior) lack of background and experience in compliance certification. By developing a software process using Moog's library of artifacts and other process assets, Skyryse can do in an 8-hour day what would otherwise have taken years of effort.

(1) Limiting inspection to search of file names and hash values is insufficient.

Similar to source code and technical documents, Moog's process assets are less likely to be copied wholesale by Skyryse employees into Skyryse systems and devices, and more likely to be used as a Moog "reference library." This is true not only because there are markers specific to Moog in these process assets (making theft too obvious from wholesale copying), but because these process assets need to be adapted to Skyryse's existing projects and systems. Skyryse employees are most likely to pick and choose what they like from these process assets, changing distinctive terms and names and otherwise obfuscating the theft as they go along.

Searching for hash values and file names are largely useless to identify such misappropriation.

(2) Moog's Retained Expert Can Conduct the Inspection Necessary, Not the Neutral Forensic Vendor

To identify misappropriation of process assets involves analyzing Skyryse's process assets to determine whether they were developed by reference to and misappropriation of Moog's process assets. For example, the retained expert must analyze Skyryse's process for generating artifacts and whether it mimics Moog's artifacts; and compare the parties' templates, checklists, and other process assets for telltale similarities. DO-178, the governing compliance standard, is very unique and particular, with prescriptive requirements for how a company develops aviation software in order to be in compliance. The retained expert needs to have knowledge of DO-178 and related compliance testing and certification procedures in order to adequately analyze the process assets. To determine whether similarities between DO-178 process assets are unusual

and likely the result of copying (rather than what you might typically find in process assets) requires the right experience and the execution of informed judgment. This is not a mechanical exercise, but instead requires someone with the right expertise in aviation software development.

iDS does not have the expertise to conduct the inspection described above. iDS does not have experts in aviation software development, DO-178, and related compliance procedures and certification. (*See* Appx. Ex. E). Nor should it, because that is not a set of qualifications that iDS was screened for; and it is outside the scope of the work iDS was retained to perform. Even in a more "ordinary" case of software theft—without all the process assets described above that are so specific to government regulations in the aviation industry—parties routinely rely on experts with specific source code and industry experience to conduct reviews and inspections. Here, iDS cannot fulfill the role necessary in order to uncover the misappropriation at the heart of this case.

Defendants suggested during the parties' meet and confer on April 15 that they might be willing to produce all the process assets, source code, and technical documents to Moog was review, separate from the forensic images themselves. This is not acceptable for at least the following reasons:

First, Defendants have shown themselves incapable of or unwilling to identify responsive documents during the TRO compliance process, and there is no reason to believe that they will do any better of a job of identifying documents in this context. Defendants' unwillingness to return Moog's non-public information in compliance with the TRO has also robbed Moog of any comfort that Defendants will fully produce any particular category of documents on the 25 devices.

Second, for Defendants to identify all process assets, source code, and technical documents across 25 devices will likely take an enormous amount of time—again, due to their apparent incapability or unwillingness to conduct a diligent search and identification, and the likelihood of this process fomenting multiplicative disputes requiring Court intervention. This will inject undue delay into the case and make it virtually impossible for the parties to comply with the expedited discovery schedule.

Third, while source code, technical documents, and process assets are certainly at issue, the full scope of the ways in which Defendants have misappropriated over 1.3 million files—covering a huge swath of Moog's trade secrets—is unknown to Moog. Therefore, merely having Defendants produce certain types of information (like source code, technical documents, and process assets) is insufficient. At the very least, Moog's retained expert must be permitted to identify, through direct inspection of the forensic image of the devices, *what* has been stolen, copied, and integrated into Defendants' own documents, before Moog can craft comprehensive requests for production of specific categories of documents. Only Defendants fully know how they have misappropriated Moog's data and how they have integrated such data into their own documents. Moog should not be forced to "guess" at how they have misappropriated the data in order to provide search terms to Defendants while wearing a proverbial blindfold, but should instead be entitled to discover for itself the scope, depth, and breadth of Defendants' misappropriation. *Allergan*, 2011 WL 13323241, at *2 ("Another factor contributing to [the] analysis is the obvious fact that none of us knows what is actually contained on the sectors and fragments of the media involved. . . . Without mining through it, neither side really knows what is out there. Matters of such potential importance should not be managed based upon suggestions

or suspicions. Nor should they be approached with hit-and-miss methodology, if there is a reasonable alternative."). The source code, technical documents, and process assets, are just exemplary and only part of the picture.

iii. Forensic Data Regarding Devices

In order for Moog to determine the scope of Defendants' misappropriation, Moog's retained expert must be able to inspect forensic *data* regarding at least the 25 devices Defendants have collectively turned over to iDS, in order to follow the trail of misappropriation. This forensic data would help Moog determine, for example, exactly when those devices were connected to other devices, and the identity of the other devices. This forensic data would also help Moog determine what data from the devices were transferred onto other devices and when, and vice versa; whether any transferred Moog data migrated onto the Skyryse network (as opposed to individual employee devices); how Moog data on those devices were accessed (e.g., whether viewed, edited, etc.); when Moog data was deleted from those devices and what the deleted Moog data are; device history like date and time stamps pertaining to connections to other devices, file access histories, file download histories, file upload histories, and so forth. Much of the forensic data would be available in forensic images of the devices; but Moog would also need access to photographs of the devices, and specifications and serial number identifiers, including internal/embedded serial numbers. In sum, Moog's retained expert needs the forensic data regarding the devices to help determine what Defendants have been doing with Moog's data since at least November 2021.

Only by following this trail himself can Moog's retained expert get a complete picture of Defendants' misappropriation. *See Allergan*, 2011 WL 13323241, at *2 ("[T]he interest of the Plaintiff in attempting to discover and then follow the trail (if it exists) of materials that allegedly have been unlawfully electronically transferred and/or deleted is very high."). Defendants' proposal that Moog be limited to having iDS search for file names and hash values would not be sufficient for following the trail. *Id.* (finding that "the use of search terms to attempt to discover the suspected trails is awkward"). Moreover, given that Moog does not know what is on the devices, and Defendants have failed to provide such information, that is all the more reason to give Moog's retained expert direct access to the forensic images to determine what is on the devices. *Id.* Moog's proposal is particularly appropriate where, as here, Skyryse's employees are alleged to have stolen Moog's data by transferring them onto the devices at issue. *See id.* ("One factor contributing to the analysis is [that] it is a case involving departing employees who are alleged to have transferred protected date [sic] onto their personal storage media and also to have both deleted and further transferred it on."). Skyryse's employee, Kim, is also known to have deliberately deleted (i.e., spoliated) the data she copied from at least one hard drive and covering her tracks of theft and misappropriation. *See id.* (finding direct inspection of the device appropriate because "it is, at least in significant part, a case dealing with allegations of 'missing data' on the media in question").

Defendants suggest that iDS can conduct the above forensic inspection itself, rather than Moog's own retained expert. But that would only inject needless and unacceptable delay into the discovery schedule, with far less effective results (which is perhaps Defendants' aim). For example, it would make no sense for Moog's retained expert to provide instructions to iDS on what steps to take, have iDS take a week to execute on those steps against 25 devices and send

back the results, have Moog's retained expert review those results and tell iDS the next set of steps based on that review, have iDS take another week to execute on the new set of steps against the 25 devices, and so forth iteratively ad infinitum. That is completely inefficient and would take too long and result in a massive and unnecessary prolongation of the expedited discovery schedule. Moog's retained expert knows the case, knows what to look for, and needs to be able to conduct the inspection himself, "following the trail" and adjusting his direction and process as he goes along. Moreover, because the parties' communications with iDS should not be *ex parte*, Moog's retained expert's instructions to iDS (i.e., his work product) would become known to Defendants. This is unacceptable, not only because Defendants are not entitled to this work product but also because Defendants should invest their own resources into their own retained expert and not be able to use Moog's expert.

C. Outside Counsel Need Access to the Forensic Images as Well as Experts

While Moog's retained experts will chiefly conduct the inspection, Moog's outside counsel also need to be involved to provide input on the inspection, answer questions from the retained experts, and use the retained expert's work product in the context of the litigation. The retained experts are not lawyers, and cannot conduct an inspection in a vacuum without the assistance of outside counsel. The retained experts must be able to discuss their inspection work with outside counsel. Moreover, how a particular document on the devices bears on the parties' legal claims and defenses is a legal question, and something that outside counsel will need to analyze and determine; to do so will require, in many instances, outside counsel to look at the document in question.

On the parties' meet and confer, Defendants expressed concern that Moog's outside counsel would discuss the contents of the forensic image with Moog's in-house counsel. But Moog's protocol specifically forbids this. The materials to be hosted by iDS for inspection are, by default, designated "HIGHLY CONFIDENTIAL—OUTSIDE COUNSEL & EXPERTS' EYES ONLY" (*see* Appx. Ex. A, III.D.9) and cannot be disclosed to in-house counsel or other employees of Moog. (As noted in Moog's proposed protocol, however, to the extent a document is determined to not merit such a designation, Moog may request that Defendants produce the document under a less restrictive designation. (*See id.*, § IV).) Meanwhile, Moog's outside counsel and retained experts would only get direct access to the forensic images subject to highly restrictive protections. (*See* Appx. Ex. A, § VIII.B). There is no reason here to doubt that Moog's outside counsel, as officers of the Court, will comply with the Protective Order.

D. Conclusion

Defendants' proposed protocol—which permits only the superficial searching of file names and hash values by the neutral forensic vendor—appears designed to hobble Moog's ability to identify the egregious theft and misappropriating use that Defendants have engaged in. Defendants are in possession of (or have spoliated) nearly all the evidence of theft and misappropriation in this case, and know exactly what they took and what they have done with it—yet are attempting to erect a wall between Moog and that evidence. That is extremely concerning and, to Moog, very strong confirmation that egregious misappropriation has indeed occurred and that Defendants seek to hide it from Moog and the Court.

Moog respectfully requests that the Court enter Moog's proposed protocol, attached as Exhibit A, as the inspection protocol in this case, so that a full, fair, and effective investigation can be conducted into Defendants' misappropriation.

III. Dispute Regarding AEO Provisions

A. Moog's Proposed AEO Provision Regarding The Individual Defendants.

This case involves former Moog and current Skyryse employees Kim and Pilkington copying a total of over 1.3 million Moog files related to flight control software development and testing before leaving Moog to join its competitor Skyryse. Kim and Pilkington have admitted in discovery responses that they retained Moog Confidential Information upon beginning employment at Skyryse. (*See* Appx. Ex. F). After departing for Skyryse, Kim returned two hard drives to Moog, one of which she used to copy over 136,000 files of Moog data and had been intentionally formatted to wipe it clean. These facts are undisputed. With this backdrop, Moog has considerable concerns about wholesale disclosure of its AEO materials to the Individual Defendants and Skyryse employees.

Regarding individual defendants Pilkington and Kim, Moog makes the very reasonable proposal that Moog AEO material may be disclosed to them provided that:

- they are "a sender, recipient or author" of the material;
- any such disclosure be made "solely for a purpose related to the litigation;"
- "any such disclosure be made by counsel for the Party under circumstances whereby counsel is able to continuously observe [them] (e.g., physically or via videoconference with the camera on and facing the individual;"
- counsel "admonish [Pilkington and Kim] to refrain from taking screenshots or pictures of the material;"[10]
- Pilkington and Kim "shall not be permitted to make or retain printouts or copies" of any AEO material; and
- "any and all notes, annotations, or other records created by" Pilkington and Kim during the disclosure shall be immediately surrendered to the custody of their counsel and automatically be treated as AEO material.

(Appx. Ex. G, ¶6(j)). At the hearing on April 8, 2022, Moog announced it had reached "agreement in principle" with counsel for Pilkington and Kim that they could view AEO materials "in the presence of their counsel" that "they were authors or recipients of," as long as they did not "keep copies," and defense counsel did not object to Moog counsel's representation or otherwise raise any qualification of the parties' agreement. (*See* ECF 71 at 7:13-21). Now, counsel for the Individual Defendants seeks to backtrack on its agreement in principle.

Instead, Pilkington and Kim assert that Moog AEO material may be shown to them *regardless* of whether they were the author or recipient of the material. But this makes no sense and unfairly compromises the confidentiality of Moog AEO material. Allowing Pilkington and Kim unfettered access to all Moog AEO material even if they were ***not*** the author, addressee, or recipient of the material allows Skyryse as a direct competitor to misappropriate yet more Moog

[10] Additionally, Moog desires that this promise appear in the witness's signed undertaking and agreement to be bound, which is reasonable and consistent with the admonishment.

confidential trade secret information, and effectively nullifies a key provision of the stipulated TRO in this matter. ECF 25, ¶ 7 ("Any of Plaintiff's non-public information, documents, records, files, or data in any Defendant's possession, custody, or control (if any) ***shall not be used or reviewed by Defendants***.") (emphasis added); *Covelo Clothing, Inc. v. Atlandia Imports, Inc*., 2007 WL 4287731, at *1 (D. Colo. 2007) ("With regard to an attorneys-eyes-only provision, confidential information that may be used against the company by a direct competitor in the lawsuit is generally afforded more protection."); *Zenith Radio Corp. v. Matsushita Electric Ind. Co*., 529 F. Supp. 866, 890 (E.D. Pa. 1981) ("Competitive disadvantage is a type of harm cognizable under Rule 26."). Given Kim and Pilkington's undisputed conduct and their employment with Moog's direct competitor, Moog's proposal that Pilkington and Kim can only view Moog AEO material of which they are the sender, recipient, or author is reasonable and should be adopted by the Court.

B. Moog's Proposed AEO Provision Regarding Skyryse.

With respect to Skyryse, Moog proposes the important and additional qualifications that AEO material may only be disclosed to a Skyryse employee who "has been noticed for deposition or has been identified as a 30(b)(6) deponent to the Parties" **and** who is also "a sender, recipient or author" of the AEO material. (Appx. Ex. G, ¶6(k)). These restrictions are reasonable and necessary because Skyryse and Moog are direct competitors, and nearly one-quarter of all Skyryse employees (at least 20 out of 71 Skyryse employees) are former Moog employees. In fact, Moog is continuing its investigation and may discover that additional former Moog employees now at Skyryse have misappropriated Moog AEO material. By contrast, Moog has no former Skyryse employees on its payroll. Moog is thus at a massive competitive disadvantage vis-à-vis Skyryse with respect to the sharing of AEO material. Allowing access to Moog AEO material *only* to a Skyryse employee who has been noticed for deposition and/or identified as a 30(b)(6) witness to all parties ***and*** who is also the author, sender or recipient of the AEO material helps mitigate this competitive disadvantage and strikes the appropriate balance between protecting Moog AEO material from improper use by a direct competitor while allowing Skyryse to prepare its witnesses for deposition. *Covelo*, 2007 WL 4287731, at *1; *Zenith Radio*, 529 F. Supp. at 890.[11]

As Skyryse would have it, Moog AEO material may be disclosed to any Skyryse employee "who is the author, addressee, or recipient of the document," "who is known to have drafted all or part of the document," or "who is specifically identified in the document or its accompanying metadata," *regardless* of whether they have been noticed for deposition or identified as a 30(b)(6) witness. This makes no sense and works to Moog's severe disadvantage. First, just because a person is *referenced* or *identified* in the metadata or body of AEO material does not mean that person necessarily has knowledge of the AEO material. Moreover, just because a former Moog employee may have been an author, addressee, or recipient of Moog AEO material while at Moog does not mean they should continue to have access to such material now that their employment

[11] This is also consistent with the protective order recently entered by the Southern District of New York in *Sunlight Fin. LLC v. Samuel Duncan Hinkle*, Case No. 1:21-cv-660-JMF (S.D.N.Y. Jan. 28, 2022), Stipulated Protective Order, Dkt. 63 at ¶7.3(f) (Material designated as "Highly Confidential- Attorneys' Eyes Only" may be disclosed to "(f) the author or recipient of a document, but only for purposes of preparing that individual for his or her deposition and the individual shall not be permitted to retain any copies (hard copy of electronic) of the document(s)."). (*See* Appx. Ex. H).

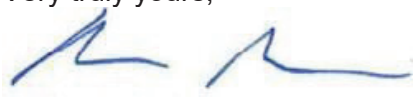
SheppardMullin

at Moog has terminated. Likewise, just because a former Moog employee may have drafted all or part of Moog AEO material while at Moog does not mean they should continue to have access to such material now that they are working for Skyryse. To the contrary, that would effectively enable Skyryse to misappropriate yet more Moog trade secret information to Moog's competitive disadvantage and would nullify the stipulated TRO in this case. *Covelo*, 2007 WL 4287731, at *1; *Zenith Radio*, 529 F. Supp. at 890; ECF 25, ¶ 7. If, as Skyryse contends, Moog AEO material is already in the minds of former Moog employees now working for Skyryse, there is no need to refresh their recollection or solidify such knowledge with access to written Moog AEO material to Moog's further detriment.

Indeed, Skyryse employees who are neither noticed for deposition nor identified as 30(b)(6) witnesses have attenuated or lesser knowledge than their colleagues who testify, *i.e.*, their knowledge is not essential in order for Skyryse to defend itself in this case. Allowing all Skyryse employees to have "unfettered access" to Moog AEO material regardless of whether they are noticed for deposition or identified as 30(b)(6) witnesses improperly "risks disclosing [Moog's] trade secrets to a person capable of competitive decision-making, precisely what the proposed AEO provision intends to prevent." *Mujae Group, Inc. v. Spotify USA Inc.*, No. 20-cv-6719, 2021 WL 3417485, at *1 (S.D.N.Y. Jun. 30, 2021). *See also J2 Global Commns., Inc. v. Protus IP Solutions*, No. 06-cv-566-DDP, 2009 WL 10671967, at *7 (C.D. Cal. Jun. 24, 2009) (rejecting the argument that a protective order prohibiting the sharing of AEO material with "witnesses [who] mainly will be former[] employees [of defendant] who have already had exposure to the confidential information and documents at issue" because "witnesses will still be able to provide testimony as to their 'actual knowledge' without reviewing confidential documents.").

Finally, Moog proposes that any and all notes, annotations, or other records created by the Party during the disclosure shall be immediately surrendered to the custody of that Party's counsel and shall automatically be treated as AEO, which is reasonable and helps ensure that Skyryse witnesses to whom Moog AEO material is disclosed do not intentionally or otherwise use such self-created notes or annotations in their job functions for Skyryse to Moog's competitive detriment. *See, United States v. Ayyad*, 2020 WL 6801911, at *1 (S.D.N.Y. Nov. 19, 2020) (ordering, among other things, that the "defendant shall not make or retain any notes that include any Highly Confidential Information outside the offices of defense counsel."). For these reasons, Moog's proposed AEO provisions as to Skyryse employees should be adopted by the Court.

Very truly yours,



Rena Andoh
for SHEPPARD MULLIN RICHTER & HAMPTON LLP

SMRH:4870-7416-2460.3